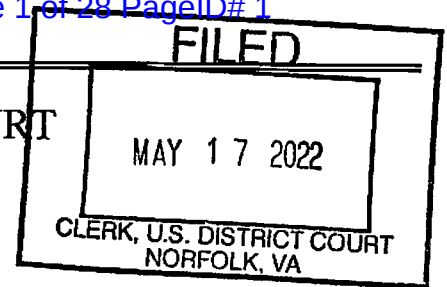


UNITED STATES DISTRICT COURT

for the  
Eastern District of Virginia



In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

THE GOOGLE ACCOUNT  
SPARKYRC1207@GMAIL.COM

Case No. 2:22sw 71

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See attachment A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252(a)(2)	Receipt of a visual depiction of a minor engaged in sexually explicit conduct
18 U.S.C. § 2252(a)(4)(B)	Possession of a visual depiction of a minor engaged in sexually explicit conduct

The application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of        days (give exact ending date if more than 30 days:       ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA:

E. Rebecca Gantt, AUSA

Printed name and title

Sworn to before me and signed in my presence.

Date: 05/17/2022

City and state: Norfolk, Virginia

  
Applicant's signature

Kathryn Nguyen, Special Agent, FBI

Printed name and title

  
Judge's signature

Lawrence R. Leonard, United States Magistrate Judge

Printed name and title

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with account **sparkyrc1207@gmail.com**, which is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

## **ATTACHMENT B**

### **Particular Things to Be Seized**

#### **I. Information to be disclosed by Google LLC (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for the SUBJECT ACCOUNT listed in Attachment A:

- a. All records or other information regarding the identification of the SUBJECT ACCOUNT or linked to the account, to include full name; physical address; telephone numbers and other identifiers;; records of session times and durations; the date on which the account was created; the length of service; the IP address used to register the account; log-in IP addresses associated with session times and dates; account status; device identifiers associated with any device that has logged into this account or device that has been linked to this account; alternative email addresses or phone numbers provided during registration; account recovery methods including any form of contact information provided; methods of connecting; log files; and means and source of payment (including any credit or bank account number);
- b. All files and backup files stored in Google Drive or elsewhere in the SUBJECT ACCOUNT, including associated data such as application data call history; device settings; contacts; calendar information; short message system files consisting of date, time, sender, receiver, and message content; photos; and videos;
- c. Cellular device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the SUBJECT ACCOUNT;
- d. Contacts—All contacts stored by Google including name, all contact phone numbers, emails, social network links, and images;
- e. All Chrome data including autofill, bookmarks, browser history, extensions, dictionary, search engine, and sync settings;

- f. Gmail—All email messages, including inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages shall include all information such as the date, time, IP address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the “cc” (carbon copy) or the “bcc” (blind carbon copy), the message content or body, and all attached files;
- g. Google Photos—All images, graphic files, video files, and other media files stored in the Google Photos service, including all associated data, such as dates of uploads, downloads, and deletion of such files;
- h. Google Maps—All Google Maps data including commute routes, commute settings, and labeled places;
- i. Google Location History/Google Timeline data for any devices associated with the SUBJECT ACCOUNT, including all location data whether derived from Global Positioning System (GPS), cell site/cell tower triangulation/multilateration, precision measurement information such as timing advance or per call measurement data, Wi-Fi location, Bluetooth, or device sensors, including accelerometer, barometer, gravity, magnetic field, orientation, or proximity. Such data shall include the GPS coordinates and the dates and times of all location recordings.
- j. Play Store—All applications downloaded, installed, or purchased by the SUBJECT ACCOUNT;
- k. Web and Application history—All search history and queries, including by way of example and not limitation, World Wide Web (web) browsing, images, news, shopping, ads, videos, maps, travel, and finance, whether performed in private browsing, incognito, anonymous or secret mode, all device activity including application use, social media use, device phone functions such as calling or text messaging activity, email activity including read, sent, and received emails, and the dates and times of searches made and applications used;
- l. Voice—All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voicemail messages sent by or from the Google Voice account associated with THE SUBJECT ACCOUNT;
- m. The types of service used;

- n. All records or other information stored by an individual using the SUBJECT ACCOUNT, including address books, contact and buddy lists, calendar data, pictures, and files;
- o. All location information pertaining to the SUBJECT ACCOUNT or linked to the account; and
- p. All records pertaining to communications between the Provider and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **FOURTEEN DAYS** of issuance of this warrant.

## **II. Information to be seized by the government**

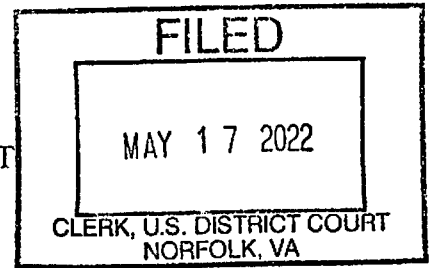
All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of the violations of 18 U.S.C. § 2252(a)(2), distribution of images of minors engaged in sexually explicit conduct; and 18 U.S.C. § 2252(a)(4)(B), possession of images of minors engaged in sexually explicit conduct, for the SUBJECT ACCOUNT listed in Attachment A, including information pertaining to the following matters:

- a. Images, videos, and other depictions of minors engaged in sexually explicit conduct and images, videos and other depictions of child erotica;
- b. Evidence reflecting the shipment, mailing, or purchase of goods and items in exchange for child pornography, including the shipment, mailing, or purchase of computers, vibrators, lingerie, and shoes, and bank, credit card, PayPal, or online merchant data associated with the exchange of money, goods, or items for child pornography;
- c. Evidence indicating how and when the SUBJECT ACCOUNT was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the SUBJECT ACCOUNT owner;
- d. Evidence indicating the SUBJECT ACCOUNT owner or user's state of mind as it relates to the crime under investigation;
- e. The identity of the person(s) who created or used the SUBJECT ACCOUNT, including records that help reveal the whereabouts of such person(s).
- f. The identity of the person(s) who communicated with the owner or user of the SUBJECT ACCOUNT about matters relating to the distribution or possession of

child pornography, including records that help reveal the whereabouts of individuals solicited, enticed, or requested to produce or transmit child pornography.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

IN THE UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF VIRGINIA  
Norfolk Division



IN THE MATTER OF THE SEARCH OF  
THE GOOGLE ACCOUNT  
SPARKYRC1207@GMAIL.COM

No. 2:22sw 71

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Special Agent Kathryn Nguyen, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for information associated with **sparkyrc1207@gmail.com**—the SUBJECT ACCOUNT—that is stored at premises controlled by Google, an email and cloud storage provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. I seek a search warrant requiring Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am an FBI Special Agent and have served in that capacity since September 2015. I am an investigator or law enforcement officer of the United States within the meaning of Rule

41(a)(2)(C) of the Federal Rules of Criminal Procedure, that is, a federal agent empowered to conduct investigations and engaged in enforcing the federal criminal statutes.

3. I am currently assigned to the Norfolk Field Office. In the course of my duties, I am responsible for investigating crimes which include, but are not limited to, child exploitation and child pornography. I have previously been involved in criminal investigations concerning violations of federal laws. Since joining the FBI, your affiant has received specialized training in human trafficking investigations, identifying and seizing electronic evidence, computer forensics, recovery of electronic files, electronic device imaging, and social media website investigations.

4. This affidavit is based on my personal observations, my training and experience, and my conversations with other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me about this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B) are presently located in the SUBJECT ACCOUNT.

#### **PERTINENT FEDERAL CRIMINAL STATUTES**

5. This warrant is sought in support of an investigation into violations of the following federal criminal statutes:

a. 18 U.S.C. § 2252(a)(2) prohibits any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any

means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. 18 U.S.C. § 2252(a)(4)(B) prohibits any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

### **JURISDICTION**

6. This Court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. § 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is “a district court of the United States” that “has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Google accepts out-of-state and out-of-district service of subpoenas, court orders, and search warrants by fax without the presence of a law enforcement officer. Accordingly, I will execute the requested search warrant by facsimile to the custodian of records at Google, and I ask that the data to be copied or obtained outside of the presence of a law enforcement officer. I

anticipate that Google will produce the requested records to me in electronic format accompanied by a signed authentication letter via e-mail or on electronic media via U.S. Mail.

7. This investigation involves offenses within the jurisdiction and proper venue of the United States District Court for the Eastern District of Virginia, as more fully articulated below.

### **PROBABLE CAUSE**

8. On March 29, 2022, a law enforcement officer acting in an undercover capacity (hereinafter the "UC") posing as the father of an 11 year-old daughter posted a description in the "about me" section on a social-networking application located on the internet. The description used language that is commonly associated with individuals seeking to find children for sexual purposes.

9. On March 29, 2022 at 5:34PM the UC received a response from Study\_WaitWhat. Study\_WaitWhat asked to switch the conversation to another application, Wickr Me, and said his name on that application was Darklike. Excerpts from the conversations between the UC and subject are provided below:

#### Excerpts from Wickr Me Messages

darklike:	So tell me how long yall been doing this
UC:	been like a year or so. took it super slow
darklike:	And she likes it?
UC:	yea took it real slow so she liked it
darklike:	Tell me more about yall
UC:	we are from NY and traveling down to myrtle beach
UC:	I'm Mike, 45
UC:	kylie will be 12 in the fall
UC:	hbu
darklike:	I'm Chris I'm 31, where and how long yall staying?
UC:	just for a few days we did Busch Gardens
UC:	staying in chesapeake
darklike:	Nice lol how much you looking into wanting
UC:	you mean how much cash?
darklike:	Yea

UC: 100 bucks you can have her for an hour  
darklike: Now I'm going to ask this is there anyway to prove this is all real  
UC: we can talk on the phone  
darklike: On this app  
UC: yes  
darklike: Ok  
darklike: You can call me

10. A within-application voice call then took place between another UC and Darklike during which Darklike asked the UC if his daughter was around. Darklike then asked what he believed to be the 11-year-old daughter (an additional UC) if he likes it when daddy touches her and whether she's sucked his "peepee". Darklike said he would be available at 10PM to come over.

11. The chat conversation resumed after the voice call:

Additional Excerpts from Wickr Me Messages

darklike: I forget to ask how big is she  
UC: what u mean? she's little, kinda tight  
darklike: Skinny?  
UC: kinda  
darklike: Ok  
darklike: Could I see a pic of her  
UC: totally just don't want to share a lot of pics dont want her image out there  
darklike: Gotcha  
UC: *(shared a photo an altered photo of a fully-clothed adult)*  
darklike: OMG she's so cute and sexy  
UC: thanks man i think so to  
darklike: You should totally take her to a nudist resort  
UC: hahah yea man. are there any here??  
darklike: One in ivor Virginia called whitetails  
UC: cool  
darklike: It's family friendly and I've see sexy kids there and OMG tan kids are beautiful  
UC: might have to consider it for our next trip  
darklike: Lol I'm going to try this summer so hopefully we can meet again  
*(shared a photo of a naked prepubescent female child spreading her legs with her genitalia clearly visible)*

UC: nice love it  
UC: she yours?  
darklike: No . . .  
darklike: Has she seen a cock?  
UC: yea i've had her touch my cock but was easing into it  
darklike: If I send a pic of mine can you show her it  
UC: that would be cool and she will know what to expect when you get here  
UC: are you big?  
darklike: Average 5.5  
(shared a photo of an erect adult male penis)  
darklike: Be right back taking a shower now  
UC: k  
darklike: What does she think  
UC: she really like it  
UC: not gonna lie bigger than me lol  
darklike: Lol well I'm glad she likes it and eh I think I'm small myself  
darklike: Haha I keep looking at her pic and so badly want to jerk and cum but I also want to wait till I see her to really cum  
UC: cool save it up  
darklike: Have you cum on her before  
UC: just on the outside  
darklike: Well yea but how was her reaction and where did you cum cause I'll be honestly I would either cum on her pussy or chest and lick it clean  
UC: i did it on her chest, it would be hot to see you cum on her pussy  
darklike: Then I will lol  
UC: cool u still thinkin like 10?  
darklike: Yea somewhere between 10 and 1030  
UC: ok cool u want her showered?  
darklike: Sure  
UC: k cool shes hoppin in now. if ten works then cool shes gonna be cranky as fuck lol  
darklike: Lol well I'm sure we can make her happy then cranky  
darklike: Ask her if she wants something sweet  
UC: she would love that, her favorite candy is swedish fish  
darklike: Ok definitely will do that for her  
UC: ill have her wear her favorite unicorn onesie  
darklike: Will she be naked underneath it  
UC: definitely  
darklike: Lol I'll be honest I'm going to give you \$200 cause I can't believe that this will happen  
UC: very cool bro  
darklike: Could I stay little longer then an hour  
UC: if you can come earlier you can stay for a couple of hours

UC: she has to go to bed soon  
 darklike: I'll try 930  
 UC: great  
 darklike: Where are yall staying at  
 (*conversation confirming location of UC in Chesapeake, Virginia*)  
 darklike: On my way  
 UC: cool  
 darklike: I'm excited and little nervous haha  
 UC: same here  
 UC: it'll be fun  
 darklike: Lol why you nervous  
 darklike: Oh yea  
 UC: more nervous excited  
 darklike: Haha yea  
 darklike: She's so sexy  
 UC: yea she is  
 darklike: Almost there just got to get candy  
 UC: Great  
 darklike: They don't have any Swedish fish, what else does she like  
 UC: twix  
 darklike: Ok  
 darklike: I'm here

12. On March 29, 2022 at approximately 9:52 PM, an adult male later identified as Christafer Douglas FRIEND arrived at the Chesapeake, Virginia location where he had made arrangements to meet "Mike" and his daughter "Kylie". FRIEND brought with him the \$200 he had told the UC he would pay him to spend time with his daughter. After he gave the \$200 to "Mike," the UC, he was arrested. Agents found Twix candy on his person.

13. After being notified of his rights pursuant to *Miranda v. Arizona*, FRIEND agreed to speak with agents after his arrest and admitted to being the individual who had been corresponding with the UC. He provided the agents with his Google email, sparkyrc1207@gmail.com. He also said that his Google account synchronizes with another Internet electronic storage application, Mega, and that he uses Mega to obtain images of minors

engaging in sexually explicit conduct. In addition, during a review of FRIEND's Google Photo account, images depicting minors engaging in sexually explicit conduct were observed.

14. Agents seized his smartphone (which was on his person) and his laptop (in his vehicle). FRIEND consented to a search of both items. The smartphone contained several folders in the photo gallery, to include: "Boys Cocks", which contained 85 files, with approximately 82 images of child pornography; "Wife", which contained 4 files of child pornography; and "Child Porn", which contained 282 files, with approximately 276 images of child pornography. Approximately 45 videos of child pornography were also stored on the device.

15. FRIEND also signed a consent form authorizing agents to search his Google account. However, access to the SUBJECT ACCOUNT via his smartphone has since locked out, and the password FRIEND provided for the SUBJECT ACCOUNT is inaccurate, so agents are unable to access the SUBJECT ACCOUNT. Additionally, the instant search warrant would provide data that is unavailable through accessing the SUBJECT ACCOUNT as a user, such as historical login and location data. Additionally, Google will not provide content of an account without a search warrant. A preservation letter for the SUBJECT ACCOUNT was submitted to Google on April 6, 2022.

16. Google necessarily requires use of the Internet. The Internet is an interconnected network of computers with which one communicates when on-line, is a network that crosses state and national borders, and is a facility of interstate and foreign commerce.

17. On March 30, 2022, U.S. Magistrate Judge Robert J. Krask signed a criminal complaint charging FRIEND with attempted coercion and enticement of a minor, 18 U.S.C. § 2422(b), distribution of child pornography, 18 U.S.C. § 2252(a)(2), and attempted transfer of obscene material to a minor, 18 U.S.C. § 1470. Case No. 2:22-cr-42, ECF No. 3. On April 4,

2022, U.S. Magistrate Judge Lawrence R. Leonard entered a finding of probable cause and granted the government's motion to detain FRIEND pending trial. ECF Nos. 16 & 17. On April 20, 2022, a federal grand jury returned an indictment charging FRIEND with attempted sex trafficking of a minor, 18 U.S.C. § 1591(a)(1), attempted coercion and enticement of a minor, 18 U.S.C. § 2422(b), distribution of images depicting minors engaging in sexually explicit conduct, 18 U.S.C. § 2252(a)(2), possession of images depicting minors engaging in sexually explicit conduct, 18 U.S.C. § 2252(a)(4)(B), and attempted transfer of obscene material to a minor, 18 U.S.C. § 1470.

### **BACKGROUND CONCERNING GOOGLE**

18. Based upon my training and experience, as well as information acquired from other law enforcement officials with technical expertise, I have learned the following information about Google. Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com, like the SUBJECT ACCOUNT. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Google maintains information about the mobile devices associated with the user's Google account. This includes the make, model, and unique serial numbers of all linked devices. Google also maintains information about their customers including the primary email addresses, secondary email addresses for account password recovery, applications, websites, and services that are allowed to access the user's Google account or use the user's Google account as a password login, and account login activity such as the geographic area where the user logged into the account, what type of internet browser and device they were using, and the internet protocol (IP) address they logged in from. The IP address is roughly analogous to a telephone number assigned to a computer by an internet service provider. The IP address can be resolved back to a physical address such as a

residence or business with Wi-Fi access or residential cable internet. I believe this information will assist in the investigation by identifying previously unknown email accounts, previously unknown devices used by the suspect, and location history information tending to show the movements of the suspect and his mobile device(s).

19. Google users can enroll cellular devices with an associated Google account into a device backup service. This backup service duplicates some of the information stored on the device in the event the user loses their device, or it becomes otherwise inoperable. Device backup data is limited to data from applications stored on the device, all history including dialed, received, and missed calls, and device settings. The backup files are named with the device's manufacturer and model number in the user's Google Drive service.

20. A Google subscriber can store not only emails, but also files such as address books, favorite locations, contact or buddy lists, calendar data, pictures, and videos (other than ones attached to emails) on servers maintained or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, emails in the account, and attachments to emails, including pictures and files, as well as in location history.

21. Google Maps is a web service and application that allows users to search for places and routes to navigate using public transportation, vehicles, or bicycles or by walking. Users can label or designate specific places in Google such as home or work. Google Maps also records commute routes and commute settings based on recorded patterns such as date and time, origin and destination, and route traveled.

22. Chrome is an internet browser developed and distributed by Google. The Chrome browser is tightly integrated with other Google products and can be installed on cellular phones.

The Chrome browser collects and stores information that is transmitted to Google and retained by the company. This information includes autofill and auto-populate data from prior searches, bookmarked webpages, browser history showing searched-for words, extensions and add-ons that are developed by Google and third-parties to bring custom features to the browser, search engines used, and sync settings so the user can have the previously listed features across multiple devices. I believe this information would show FRIEND's internet activity in the days prior to his arrest and may provide further evidence of his interest in child pornography.

23. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

24. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service used, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect account usage.

25. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

26. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling law enforcement to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described above, email providers typically log the IP addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account

owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime) or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

27. Searching for the evidence described in this warrant application may require a range of data analysis techniques. In some cases, law enforcement officers and computer analysts may be able to conduct carefully targeted searches to locate evidence without needing to carry out a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Numerous types of user information and metadata stored on a cell phone are not susceptible to "word search" or similar forensic techniques, including images, audio and video recordings, and proximate GPS locations. In addition, the complex interrelatedness of cell-phone data may undermine the efficacy of narrow search techniques based on the type, location, or date of information. Indeed, the vast array of apps now available on cell phones make it difficult to determine the exact form and organization of user information and metadata prior to conducting a search. Finally, criminals can mislabel, misspell, or hide information; encode communications to avoid using key words; attempt to delete information to evade detection; or take other steps designed to frustrate law enforcement searches for information.

28. Accordingly, law enforcement officials or other analysts with appropriate expertise may need to conduct more extensive searches not obviously related to the evidence described in

this warrant application or peruse all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, FBI and its partners intend to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in this warrant application.

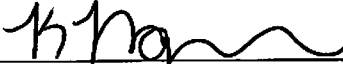
29. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

#### **CONCLUSION**

30. Based on the above, there is probable cause to believe that the SUBJECT ACCOUNT has been used in the commission of crimes and constitute evidence, fruits, and instrumentalities of violations of federal laws of the United States, including 18 U.S.C. § 2252(a)(2), distribution of images depicting minors engaged in sexually explicit conduct; and 18 U.S.C. § 2252(a)(4)(B), possession of images depicting minors engaged in sexually explicit conduct. Probable cause also exists to believe that evidence, fruits, and instrumentalities of these violations will be found in the SUBJECT ACCOUNT.

31. Because the warrant will be served on Google electronically or by mail, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

FURTHER YOUR AFFIANT SAYETH NOT.

  
\_\_\_\_\_  
Special Agent Kathryn Nguyen  
Federal Bureau of Investigation

Sworn and subscribed to before me this 17<sup>th</sup> day of May, 2022.

  
\_\_\_\_\_  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with account **sparkyrc1207@gmail.com**, which is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

## **ATTACHMENT B**

### **Particular Things to Be Seized**

#### **I. Information to be disclosed by Google LLC (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for the SUBJECT ACCOUNT listed in Attachment A:

- a. All records or other information regarding the identification of the SUBJECT ACCOUNT or linked to the account, to include full name; physical address; telephone numbers and other identifiers;; records of session times and durations; the date on which the account was created; the length of service; the IP address used to register the account; log-in IP addresses associated with session times and dates; account status; device identifiers associated with any device that has logged into this account or device that has been linked to this account; alternative email addresses or phone numbers provided during registration; account recovery methods including any form of contact information provided; methods of connecting; log files; and means and source of payment (including any credit or bank account number);
- b. All files and backup files stored in Google Drive or elsewhere in the SUBJECT ACCOUNT, including associated data such as application data call history; device settings; contacts; calendar information; short message system files consisting of date, time, sender, receiver, and message content; photos; and videos;
- c. Cellular device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the SUBJECT ACCOUNT;
- d. Contacts—All contacts stored by Google including name, all contact phone numbers, emails, social network links, and images;
- e. All Chrome data including autofill, bookmarks, browser history, extensions, dictionary, search engine, and sync settings;

- f. Gmail—All email messages, including inbox messages whether read or unread, sent mail, saved drafts, chat histories, and emails in the trash folder. Such messages shall include all information such as the date, time, IP address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the “cc” (carbon copy) or the “bcc” (blind carbon copy), the message content or body, and all attached files;
- g. Google Photos—All images, graphic files, video files, and other media files stored in the Google Photos service, including all associated data, such as dates of uploads, downloads, and deletion of such files;
- h. Google Maps—All Google Maps data including commute routes, commute settings, and labeled places;
- i. Google Location History/Google Timeline data for any devices associated with the SUBJECT ACCOUNT, including all location data whether derived from Global Positioning System (GPS), cell site/cell tower triangulation/multilateration, precision measurement information such as timing advance or per call measurement data, Wi-Fi location, Bluetooth, or device sensors, including accelerometer, barometer, gravity, magnetic field, orientation, or proximity. Such data shall include the GPS coordinates and the dates and times of all location recordings.
- j. Play Store—All applications downloaded, installed, or purchased by the SUBJECT ACCOUNT;
- k. Web and Application history—All search history and queries, including by way of example and not limitation, World Wide Web (web) browsing, images, news, shopping, ads, videos, maps, travel, and finance, whether performed in private browsing, incognito, anonymous or secret mode, all device activity including application use, social media use, device phone functions such as calling or text messaging activity, email activity including read, sent, and received emails, and the dates and times of searches made and applications used;
- l. Voice—All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voicemail messages sent by or from the Google Voice account associated with THE SUBJECT ACCOUNT;
- m. The types of service used;

- n. All records or other information stored by an individual using the SUBJECT ACCOUNT, including address books, contact and buddy lists, calendar data, pictures, and files;
- o. All location information pertaining to the SUBJECT ACCOUNT or linked to the account; and
- p. All records pertaining to communications between the Provider and any person regarding the SUBJECT ACCOUNT, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **FOURTEEN DAYS** of issuance of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of the violations of 18 U.S.C. § 2252(a)(2), distribution of images of minors engaged in sexually explicit conduct; and 18 U.S.C. § 2252(a)(4)(B), possession of images of minors engaged in sexually explicit conduct, for the SUBJECT ACCOUNT listed in Attachment A, including information pertaining to the following matters:

- a. Images, videos, and other depictions of minors engaged in sexually explicit conduct and images, videos and other depictions of child erotica;
- b. Evidence reflecting the shipment, mailing, or purchase of goods and items in exchange for child pornography, including the shipment, mailing, or purchase of computers, vibrators, lingerie, and shoes, and bank, credit card, PayPal, or online merchant data associated with the exchange of money, goods, or items for child pornography;
- c. Evidence indicating how and when the SUBJECT ACCOUNT was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the SUBJECT ACCOUNT owner;
- d. Evidence indicating the SUBJECT ACCOUNT owner or user's state of mind as it relates to the crime under investigation;
- e. The identity of the person(s) who created or used the SUBJECT ACCOUNT, including records that help reveal the whereabouts of such person(s).
- f. The identity of the person(s) who communicated with the owner or user of the SUBJECT ACCOUNT about matters relating to the distribution or possession of

child pornography, including records that help reveal the whereabouts of individuals solicited, enticed, or requested to produce or transmit child pornography.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.